

NIALL P. McCARTHY (SBN 160175)
nmccarthy@cpmlegal.com
ANDREW F. KIRTLEY (SBN 328023)
akirtley@cpmlegal.com
OWAIS M. BARI (SBN 321954)
obari@cpmlegal.com
GIA JUNG (SBN 340160)
gjung@cpmlegal.com

COTCHETT, PITRE & McCARTHY, LLP
San Francisco Airport Office Center
840 Malcolm Road, Suite 200
Burlingame, California 94010
Telephone: (650) 697-6000
Fax: (650) 697-0577

EDWARD J. WYNNE (SBN 165819)
Ewynne@wynnelawfirm.com
GEORGE R. NEMIROFF (SBN 262058)
Gnemiroff@wynnelawfirm.com
WYNNE LAW FIRM
80 E. Sir Francis Drake Blvd., Suite 3G
Larkspur, CA 94939
Telephone: (415) 461-6400
Fax: (415) 461-3900

MATTHEW RIGHETTI (SBN 121012)
matt@righettilaw.com

RIGHETTI GLUGOSKI, P.C.
The Presidio of San Francisco
220 Halleck Street, Suite 220
San Francisco, CA 94129
Telephone: (415) 983-0900

Attorneys for Plaintiffs and the Proposed Class

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

**STEVE LANDI, RICHARD E. HURLEY,
and NILA HURLEY, on behalf of themselves
and all others similarly situated,**

Plaintiffs,

V.

**PROGRESS SOFTWARE CORPORATION;
PENSION BENEFIT INFORMATION, LLC,
dba PBI RESEARCH SERVICES; and
THE BERWYN GROUP, INC..**

Defendants.

Case No.

CLASS ACTION COMPLAINT:

1. Negligence
2. Violations of the California Consumer Privacy Act (Civ. Code § 1798.150)
3. Violations of the California Unfair Competition Law (Bus. & Prof. Code § 17200, et seq.)
4. Violations of the California Customer Records Act (Civ. Code § 1798.82)
5. Declaratory Relief

DEMAND FOR JURY TRIAL

Class Action Complaint

Landi, et al. v. Progress Software Corp., et al.



TABLE OF CONTENTS

2		Page
3	I. INTRODUCTION.....	1
4	II. JURISDICTION, VENUE, AND INTRADISTRICT ASSIGNMENT.....	2
5	III. PARTIES	2
6	A. Plaintiffs	2
7	B. Defendants	4
8	IV. FACTUAL ALLEGATIONS.....	4
9	V. CLASS ALLEGATIONS	9
10	VI. CAUSES OF ACTION	13
11	FIRST CAUSE OF ACTION	13
12	Negligence	
13	SECOND CAUSE OF ACTION	16
14	Violations of the California Consumer Privacy Act (Cal. Civ. Code § 1798.150)	
15	THIRD CAUSE OF ACTION	17
16	Violations of the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, et seq.)	
17	FOURTH CAUSE OF ACTION	18
18	Violations of the California Customer Records Act (Cal. Civ. Code § 1798.82)	
19	FIFTH CAUSE OF ACTION	19
20	Declaratory Relief	
21	VII. PRAYER FOR RELIEF.....	21
22	VIII. JURY DEMAND.....	22

1 Plaintiffs Steve Landi, Richard E. Hurley, and Nila Hurley (collectively, “Plaintiffs”), on
 2 behalf of themselves and all others similarly situated, file this Class Action Complaint against
 3 Defendants Progress Software Corporation (“PSC”), Pension Benefit Information, LLC dba PBI
 4 Research Services (“PBI”), and The Berwyn Group, Inc. (“Berwyn”) (collectively, “Defendants”),
 5 and allege as follows based on personal knowledge as to their own actions, and upon information
 6 and belief as to all other matters.

7 **I. INTRODUCTION**

8 1. In or about May 2023, a group of Russian hackers known by the name “Clop” or
 9 “C10p” (the “Russian hackers”) found a security flaw in the widely used file transfer software
 10 MOVEit owned by Defendant PSC, and which was being used by Defendants PBI and Berwyn to
 11 transmit the personal identifiable information (“PII”) of millions of people. Because of this flaw,
 12 the Russian hackers were able to steal an enormous trove of Americans’ PII, including the PII of
 13 Plaintiffs and millions of other pensioners and beneficiaries of the California Public Employees’
 14 Retirement System (“CalPERS”) and California State Teachers’ Retirement System (“CalSTRS”).
 15 This massive theft of PII, referred to herein as the “Data Breach,” has left Plaintiffs and millions of
 16 others vulnerable at continuing and imminent risk of identity theft and a wide variety of other
 17 financial harms.

18 2. Plaintiffs are CalPERS or CalSTRS members whose PII was stolen because of the
 19 Data Breach. CalPERS and CalSTRS use the services of Defendants PBI and Berwyn
 20 (collectively, the “PBI Defendants”) to help reduce their costs and overpayments, and to manage
 21 cybersecurity risks to their members’ and beneficiaries’ PII. In providing these services, the PBI
 22 Defendants use PSC’s MOVEit file transfer software to transmit the PII of hundreds of thousands
 23 of CalPERS and CalSTRS members and beneficiaries, including Plaintiffs. Given the PII’s
 24 sensitive nature, the Defendants have a heightened duty to provide a secure digital infrastructure
 25 for transmitting and storing PII. This case is about Defendants’ catastrophic failure to fulfill that
 26 duty.

27 3. Plaintiffs bring this lawsuit as a class action, on behalf of themselves and a
 28 nationwide class and California subclass of all others similarly situated (collectively, “Class

1 Members,” as further defined herein), for negligence, declaratory relief, and violations of
 2 California’s Consumer Privacy Act (“CCPA”) (Cal. Civ. Code § 1798.150), Unfair Competition
 3 Law (“UCL”) (Cal. Bus. & Prof. Code § 17200 et seq.), and Customer Records Act (“CRA”) (Cal.
 4 Civ. Code § 1798.82). For relief, Plaintiffs seek damages, declaratory relief, equitable restitution,
 5 and injunctive relief.

6 **II. JURISDICTION, VENUE, AND INTRADISTRICT ASSIGNMENT**

7 4. The Court has original jurisdiction over this action under 28 U.S.C. § 1332 based
 8 on diversity of citizenship. The Court also has original jurisdiction over this action under the Class
 9 Action Fairness Act, 28 U.S.C. § 1332(d).

10 5. The Court has personal jurisdiction over Defendants because they do significant
 11 business in California, including by performing significant services for CalPERS and CalSTRS,
 12 which are based in California and are the PBI Defendants’ largest clients. The Court also has
 13 personal jurisdiction over Defendants because Plaintiffs’ claims arise from acts and omissions that
 14 occurred in California, and because Plaintiffs and millions of other members of the class and
 15 subclass proposed herein are California residents.

16 6. Venue is proper because Defendants engage in business activities throughout this
 17 district. A substantial part of the events and omissions giving rise to the claim occurred in this
 18 judicial district, a substantial part of the property that is the subject of the action (i.e., Plaintiffs’
 19 PII) is likewise situated in this district, and because all Plaintiffs reside in this district.

20 7. Divisional assignment to the San Francisco Division is proper because a substantial
 21 part of the events and omissions giving rise to the claims occurred in San Francisco County, where
 22 Plaintiff Landi resides, and because a substantial part of the property that is the subject of the
 23 action (i.e., Landi’s PII) is likewise situated in San Francisco County.

24 **III. PARTIES**

25 **A. Plaintiffs**

26 8. At all relevant times, Plaintiff Steve Landi has been a citizen of California, residing
 27 in San Francisco County. Mr. Landi’s retirement benefits are managed and controlled by
 28 CalPERS. His PII was subject to unauthorized access, disclosure, theft, and exfiltration as a result

1 of the Data Breach. This resulted in an invasion of his privacy interests, loss of value of his PII,
 2 and has placed him at imminent, immediate, and continuing risk of further identity theft-related
 3 harm, which is a source of worry for Landi. Mr. Landi expects that it will be necessary for him to
 4 spend time and money on credit monitoring, including the expense of a credit monitoring service
 5 as part of a reasonable effort to mitigate against such harm and will continue to incur such
 6 expenses on an ongoing basis. Plaintiff Landi filed a similar class action complaint against
 7 Defendants in San Francisco County Superior Court on June 26, 2023, but subsequently decided to
 8 seek voluntarily dismissal of his state court complaint, before any of the Defendants had been
 9 served with process in that action, in favor of re-filing in federal court via the instant Class Action
 10 Complaint.

11 9. At all relevant times, Plaintiff Richard Hurley has been a citizen of California,
 12 residing in Contra Costa County. Mr. Hurley's retirement benefits are managed and controlled by
 13 CalSTRS. His PII was subject to unauthorized access, disclosure, theft, and exfiltration as a result
 14 of the Data Breach. This resulted in an invasion of Mr. Hurley's privacy interests, loss of value of
 15 his PII, and has placed him at imminent, immediate, and continuing risk of further harm from
 16 identity theft and other misuse of his PII, which is a source of worry for Hurley. Mr. Hurley
 17 expects that it will be necessary for him to spend time and money on credit monitoring, including
 18 the expense of a credit monitoring service as part of a reasonable effort to mitigate against such
 19 harm and will continue to incur such expenses on an ongoing basis.

20 10. At all relevant times, Plaintiff Nila Hurley has been a citizen of California, residing
 21 in Contra Costa County. She is the wife of Plaintiff Richard Hurley, who has power of attorney of
 22 Mrs. Hurley because her health makes it difficult for her to manage her own affairs. Mrs. Hurley's
 23 retirement benefits are managed and controlled by CalSTRS. Her PII was subject to unauthorized
 24 access, disclosure, theft, and exfiltration as a result of the Data Breach. This resulted in an invasion
 25 of Mrs. Hurley's privacy interests, loss of value of her PII, and has placed her at imminent,
 26 immediate, and continuing risk of further harm from identity theft and other misuse of her PII,
 27 which is a source of worry for Hurley. Mrs. Hurley expects that it will be necessary for her to
 28 spend time and money on credit monitoring, including the expense of a credit monitoring service

1 as part of a reasonable effort to mitigate against such harm and will continue to incur such
 2 expenses on an ongoing basis.

3 **B. Defendants**

4 11. Defendant Progress Software Corporation (“PSC”) owns MOVEit, the software at
 5 the center of the Data Breach. PSC is incorporated in Delaware and has its principal place in
 6 Burlington, Massachusetts.

7 12. Defendant Pension Benefit Information, LLC (“PBI”), which does business as PBI
 8 Research Services, is a pension plan management services provider that is organized under the
 9 laws of Delaware and has its principal place of business in Minneapolis, Minnesota.

10 13. Defendant The Berwyn Group, Inc. (“Berwyn”) is a pension plan management
 11 services provider that is incorporated in Ohio and has its principal place of business in
 12 Independence, Ohio.

13 14. Defendants PBI and Berwyn announced that they are merging, are in the process of
 14 merging, and have operated at relevant times as a single and/or joint enterprise. They are
 15 collectively referred to herein as the “PBI Defendants.”

16 **IV. FACTUAL ALLEGATIONS**

17 15. CalPERS is the nation’s largest public pension fund, managing retirement benefits
 18 for approximately 1.9 million state and local government employees, retirees, and their families.

19 16. CalSTRS is the nation’s second-largest public pension fund with over 900,000
 20 members and beneficiaries that include current and retired public school teachers and
 21 administrators (pre-kindergarten through community college) and their families.

22 17. CalPERS and CalSTRS use members’ and beneficiaries’ PII to ensure that they are
 23 appropriately distributing pension funds to the right beneficiaries at the right time. They rely on
 24 entities like the PBI Defendants for PII verification, death audit, and locate services, as well as
 25 uncashed check management.

26 18. CalPERS and CalSTRS entrusted the PII of their members and beneficiaries to the
 27 care, custody, and control of the PBI Defendants, in material part because the PBI Defendants

represent that they rigorously protect the security of their clients' information and PII. The PBI Defendants boldly claim on their website that:

Protecting and securing the information of our clients and our company is of critical importance to PBI. We recognize that all relationships with current and prospective clients are based upon integrity and trust, and we take our role as custodians of confidential information very seriously.

19. The PBI Defendants claim on their website that they deploy a sophisticated, multi-layered approach to data security that includes but is not limited to (a) implementing secure development practices, including annual training for their IT team; (b) using real-time scanning of code changes for vulnerabilities; (c) using web application firewalls; (d) using n-tier application architecture; (e) requiring a security awareness training program for all employees at onboarding and on a regular basis thereafter; (f) using data loss prevention tools to alert and block transfers of sensitive data; and (g) using a consolidated “SIEM” solution. SIEM is a security software that gives organizations a bird’s-eye-view of activity across their entire network so they can respond more quickly to threats, before business is disrupted.

20. The PBI Defendants also claim that their data security team manages this multi-layered security architecture by performing over 30 security reviews of their quarterly audit checks to test compliance against security policies. The PBI Defendants further claim that their formalized security program follows the industry-recognized security policy frameworks from the National Institute of Science & Technology (NIST) SP 800-53 and NIST Cybersecurity Framework.

21. The PBI Defendants, in deploying this digital infrastructure, voluntarily assume responsibility for complete network security. Their website states that they regularly use third parties to test and audit their security controls, that they conduct monthly and quarterly vulnerability assessments and penetration tests of their internal and external network and application security, and that they conduct annual application penetration tests.

22. The PBI Defendants collect a significant amount of PII. Examples include individuals' full name, driver's license number, passport number, age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental

1 disability, sex, gender, gender identity, gender expression, pregnancy or childbirth and related
 2 medical conditions, sexual orientation, health insurance information, veteran or military status,
 3 insurance policy number, education, employment, employment history, bank account number,
 4 credit card number, debit card number, other financial information, browsing history, search
 5 history, history of interactions with a websites or web application, and “sensory data” (defined to
 6 include “audio, electronic, visual, thermal, olfactory, or similar information”). The PBI Defendants
 7 collect this information from sources that include government sources, such as state, local, and
 8 federal government entities. Their stated purpose for collecting this information is “preventing
 9 fraud or avoiding overpayment of benefits to deceased individuals.”

10 23. As part of their digital infrastructure, the PBI Defendants use a data transfer
 11 software called MOVEit to transmit PII and other data both within the company and with their
 12 clients.

13 24. MOVEit is owned by Defendant PSC, which claims on its website that
 14 “performance, reliability and security are at the heart of everything we [PSC] design;” that
 15 MOVEit allows users “to securely exchange information”; and that using MOVEit will “[e]xtend
 16 file transfer capabilities to all users to eliminate insecure use of email” and “[r]educe the risk of
 17 data loss and non-compliance with a fully-auditable and managed file transfer solution.”

18 25. Whatever PSC’s claims, they could not absolve the PBI Defendants of their
 19 responsibility to make good on their own promises to protect and secure the PII and other sensitive
 20 information entrusted to PSC’s custody, care, and control. If the PBI Defendants had actually
 21 performed the rigorous audits, testing, third-party stress tests, and encryption tools that they
 22 advertised to their customers on their website and elsewhere, they would have detected the security
 23 vulnerabilities in MOVEit and either eliminated those vulnerabilities or open to use a safer
 24 software.

25 26. At all relevant times, Plaintiffs’ and Class Members’ PII was being shared and
 26 transferred using MOVEit in the PBI Defendants’ digital infrastructure.

27 27. In or about May 2023, the Russian hackers involved in the Data Breach discovered
 28 a Structured Query Language (“SQL”) vulnerability in the MOVEit software. Despite all the

1 Defendants' promises of proactive data and network security efforts, none of the Defendants
 2 detected this flaw. The Russian hackers used this flaw in MOVEit to steal millions of individuals'
 3 PII, including PII in the possession, custody, and control of the PBI Defendants. Subsequent
 4 reporting has indicated that the Data Breach result in the theft of PII and other sensitive data not
 5 just from the PBI Defendants, but from hundreds of other organizations.

6 28. In a statement on its website, PSC admitted that hackers had discovered and
 7 exploited a "zero-day vulnerability" in its MOVEit software. This phrase refers to an undetected
 8 vulnerability to which PSC's security systems had zero days to respond.

9 29. PSC further admitted on its website that:

10 a SQL injection vulnerability has been found in the MOVEit Transfer
 11 web application that could allow an unauthenticated attacker to gain
 12 access to MOVEit Transfer's database. An attacker may be able to
 13 infer information about the structure and contents of the database and
 14 execute SQL statements that alter or delete database elements,
 15 depending on the database engine being used (MySQL, Microsoft
 16 SQL Server, or Azure SQL). NOTE: this is exploited in the wild in
 17 May and June 2023; exploitation of unpatched systems can occur via
 18 HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five
 19 explicitly mentioned versions are affected, including older
 20 unsupported versions.

21 30. The Data Breach occurred due to Defendants' negligence, recklessness, and other
 22 unlawful and unfair conduct in failing to take reasonable steps necessary to secure Plaintiffs' and
 23 Class Members' PII. The Data Breach was a direct and proximate result of Defendants' (i) failure
 24 to implement appropriate security measures, (ii) failure to conduct adequate security testing and
 25 stress testing to discover vulnerabilities in the MOVEit software , and (iii) breach of their express
 26 promises and guarantees concerning the reliability and security of the MOVEit software and the
 27 PBI Defendants' digital infrastructure.

28 31. Defendants kept Plaintiffs' and Class Members' highly sensitive PII in a digital
 29 infrastructure that lacked adequate security, making it unreasonably vulnerable to unauthorized
 30 access by cybercriminals.

31 32. As a result of Defendants' acts and omissions, Plaintiffs and Class Members' PII in
 32 the form of full names, social security numbers, dates of birth, and zip codes were accessed and

1 stolen by unauthorized third parties. Reporting and communications from CalPERS and CalSTRS
 2 have indicated that the PII of some of their members' former and current employers, spouses,
 3 domestic partners, and children were also accessed and stolen.

4 33. Despite the Data Breach having occurred on or about in the last week of May 2023,
 5 and despite the PBI Defendants becoming aware of the Data Breach no later than May 27, 2023,
 6 the PBI Defendants did not inform CalPERS that there had been a data security incident affecting
 7 their members' PII until June 4, 2023. On June 8, 2023, the PBI Defendants representatives
 8 formally confirmed that PII of CalPERS members had been affected by the Data Breach.

9 34. CalPERS and CalSTRS members and beneficiaries are typically senior citizens,
 10 who are prime targets for identity theft and financial scams. As a result of Defendants' lax
 11 security, hackers have accessed these members' and beneficiaries' PII in an unencrypted,
 12 unredacted, and otherwise readily usable form that is of great value to criminals, who can and do
 13 use it to cause Plaintiffs' and Class Members' PII to be accessed by criminals seeking to use it for
 14 illegal activities, such as identity theft schemes.

15 35. PII is valuable to criminals, as evidenced by the prices they will pay for PII on the
 16 dark web. On information and belief, PII and banking information can be sold at a price ranging
 17 from \$40 to \$200 per record per person on the dark web.

18 36. At all relevant times, Defendants knew, or reasonably should have known, of the
 19 importance of protecting PII and the consequences of a data breach, including the significant
 20 privacy and economic harms that foreseeably would be, and have been, imposed on Plaintiffs and
 21 Class Members. Because of the Data Breach, Plaintiffs and Class Members face an increased risk
 22 of identity theft. As a result, Plaintiffs and Class Members require robust credit monitoring
 23 services and software to reasonably mitigate the danger of future identity theft and fraud.

24 37. Defendants' acts and omissions have caused and will continue to cause Plaintiffs
 25 and Class Members to be in stress, anger, and worry, and to fear for the security of their PII and
 26 financial security and safety.

1 **V. CLASS ALLEGATIONS**

2 38. This action is brought by Plaintiffs individually and as a class action under
 3 Federal Rule of Civil Procedure (“Rule”) 23(a), 23(b)(2), 23(b)(3), and/or 23(c)(4), on behalf of
 4 themselves and the following nationwide class of similarly situated persons (the “Class”):

5 All persons residing in the United States whose nonencrypted or
 6 nonredacted personal information was subject to unauthorized access
 7 and exfiltration, theft, or disclosure, as a result of the Data Breach, as
 defined herein.

8 39. In the alternative, Plaintiffs bring this case as a class action under Rule 23(a),
 9 23(b)(2), 23(b)(3), and/or 23(c)(4), on behalf of themselves and the following subclasses of
 10 similarly situated persons (the “Subclasses”):

11 ***California Subclass.*** All persons residing in California whose
 12 nonencrypted or nonredacted personal information was subject to
 13 unauthorized access and exfiltration, theft, or disclosure, as a result of
 the Data Breach, as defined herein.

14 ***CalPERS Subclass.*** All persons who are a CalPERS member or
 15 beneficiary, and whose nonencrypted or nonredacted personal
 16 information was subject to unauthorized access and exfiltration, theft,
 or disclosure, as a result of the Data Breach, as defined herein.

17 ***CalSTRS Subclass.*** All persons who are a CalSTRS member or
 18 beneficiary, and whose nonencrypted or nonredacted personal
 19 information was subject to unauthorized access and exfiltration, theft,
 or disclosure, as a result of the Data Breach, as defined herein.

20 40. Excluded from the Class and Subclasses are the following individuals and entities:
 21 Defendants and their parents, subsidiaries, affiliates, officers and directors, current or former
 22 employees, and any entity in which Defendants have a controlling interest; all individuals who
 23 make a timely election to be excluded from this proceeding using the correct protocol for opting
 24 out; any and all federal, state, or local governments, including but not limited to their departments,
 25 agencies, divisions, bureaus, boards, sections, groups, counsels, and subdivisions; all judges
 26 assigned to hear any aspect of this litigation, as well as their staff and immediate family members;
 27 and any counsel or any party to this litigation.

1 41. Plaintiffs reserve the right to amend or modify the proposed definitions of the Class
 2 and Subclasses and to add one or more subclasses based on information obtained during this
 3 litigation.

4 42. All persons who are members of the proposed Class ("Class Members"), which
 5 includes but is not limited to all members of the proposed Subclasses, have suffered injury during
 6 the applicable limitations period, or are realistically threatened with future or ongoing injury,
 7 caused by Defendants' wrongful acts and omissions alleged herein.

8 43. This action is properly brought and may be properly maintained as a class action
 9 against Defendants pursuant to the following provisions of Rule 23:

10 a. **Numerosity (Rule 23(a)(1)):** The members of the Class and Subclasses are
 11 each in the hundreds of thousands of persons, and thus are so numerous that joinder of all members
 12 is impracticable.

13 b. **Commonality and Predominance (Rule 23(a)(2) and 23(b)(3)):** There are
 14 questions of law and fact common to the members of the Class that predominate over any
 15 questions affecting only individual members, including:

- 16 i. Whether Defendants' owed Plaintiffs and Class Members a duty to
 17 take reasonable steps to protect Plaintiffs' and Class Members' PII
 18 from unauthorized access and exfiltration, theft, or disclosure;
- 19 ii. Whether Defendants breached of this duty;
- 20 iii. Whether Defendants' negligence was a substantial factor in causing
 21 the Data Breach or the extent of the resulting harm to Plaintiffs and
 22 Class Members;
- 23 iv. Whether Plaintiffs and Class Members were injured by Defendants'
 24 conduct complained of herein;
- 25 v. Whether Defendants' conduct violated the CCPA;
- 26 vi. Whether Defendants' conduct violated the CRA;
- 27 vii. Whether Defendants' conduct violated the UCL;

- viii. Whether Defendants' conduct was a substantial factor in causing Plaintiffs' and Class Members' damages;
- ix. Whether Defendants failed to timely provide legally required notice of the Data Breach;
- x. Whether the Court should enter declaratory relief in favor of Plaintiffs and Class Members;
- xi. Whether Plaintiffs and Class Members are entitled to preliminary or permanent injunctive relief;
- xii. Whether Plaintiffs and Class Members are entitled to compensatory, punitive, or other damages; and
- xiii. Whether Plaintiffs and Class Members are entitled to equitable restitution.

c. **Typicality (Rule 23(a)(3)):** Plaintiffs' claims are typical of those of all other Class Members. Plaintiffs, like all other Class Members, sustained economic and other injury as a result of Defendants wrongful acts and omissions, which were a substantial factor in causing all of their nonencrypted or nonredacted personal information to be subject to unauthorized access and exfiltration, theft, or disclosure in the Data Breach. Plaintiffs and Class Members were and are similarly or identically harmed by the same wrongful conduct of Defendants.

d. **Adequacy of Representation (Rule 23(a)(4)):** Plaintiffs will fairly and adequately represent and protect the interests of all Class Members and have retained competent and qualified counsel with extensive experience in data breach and consumer class action litigation. There are no material conflicts between the claims of the Plaintiffs and the Class Members that would make class certification inappropriate. Counsel for Plaintiffs and the putative Class will vigorously prosecute the claims of all putative Class Members and are willing and prepared to serve the Court and the putative Class in a representative capacity.

44. This action is properly brought and may be properly maintained as a class action pursuant to Rule 23(b) for the following reasons:

a. **Class Action Status (Rule 23(b)(1)):** Class action status is appropriate under Rule 23(b)(1)(A) because prosecution of separate actions by each of the thousands of persons who are Class Members would create a risk of establishing incompatible standards of conduct for Defendants and inconsistent results for the Class Members. Class action status is also appropriate under Rule 23(b)(1)(B) because prosecution of separate actions by individual Class Members would create a risk of adjudication with respect to those individual Class Members that, as a practical matter, would be dispositive of the interests of other Class Members or would substantially impair or impede those other Class Members' ability to protect their interests.

b. **Declaratory and Injunctive Relief (Rule 23(b)(2)): Certification under Rule 23(b)(2) is appropriate because Defendants, on the same or substantively similar grounds, violated Class Members' common law and statutory rights, thereby making appropriate final injunctive, declaratory, or other appropriate equitable relief with respect to the Class as a whole.**

c. **Predominance and Superiority (Rule 23(b)(3)):** Certification of the Class and Subclasses under Rule 23(b)(3) is appropriate because questions of law or fact common to Class Members and Subclass Members, including but not limited to those questions listed above, predominate over any questions affecting only individual members of the Class or Subclasses, and because class action treatment is superior to the other available methods for the fair and efficient adjudication of this controversy, for the following non-exhaustive reasons:

- i. Given the various legal issues involved in this action, the expense of litigating the claims, and the relatively small amounts of money at issue for each Class Member, few, if any, Class Members would decide to seek, or could afford to seek, legal redress for the wrongs that Defendants have committed against them individually, and absent Class Members have no substantial interest in individually controlling the prosecution of individual actions;
- ii. This action will ensure an orderly and expeditious administration of Class Members' claims and foster economies of time, effort, and expense, and ensure uniformity of decisions;

- iii. Without a class action, Class Members will continue to suffer injury, and Defendants' unlawful conduct will continue;
- iv. This action does not present any undue difficulties that would impede its management by the Court as a class action; and
- v. The injuries suffered by individual Class Members are relatively small compared to the burden and expense of individual prosecution needed to address Defendants' wrongful conduct alleged herein. Individualized litigation presents a potential for inconsistent or contradictory judgments. In contrast, a class action presents far fewer management difficulties; allows the hearing of claims that might otherwise go unaddressed; and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

14 45. **Issue Certification (Rule 23(c)(4)):** Certification of issues of liability and
15 declaratory, equitable, and legal relief under Rule 23(c)(4) is appropriate because these issues are
16 common to all Class Members, including but not limited to whether Defendants' conduct violated
17 their common law or statutory obligations to Plaintiffs and Class Members, and whether said
18 conduct was a substantial factor in causing Class Members' harms. Resolution of such common
19 issues on a class-wide basis will materially advance the disposition of the litigation as a whole.

20 46. The Class Members are ascertainable from Defendants' own records, and there is a
21 well-defined community of interest in the questions of law or fact alleged herein since Defendants
22 violated the rights of each Class Member in the same or similar fashion.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence

26 47. Plaintiffs re-allege each of the allegations set forth in the preceding paragraphs.

27 48. Defendants owed Plaintiffs and Class Members, under both the law of negligence
28 and negligence per se, a duty to exercise reasonable care preventing their nonredacted and

1 unencrypted PII from access and exfiltration, theft, or disclosure by unauthorized third parties. The
 2 duties owed by Defendants to Plaintiffs and Class Members include, but are not limited to, the
 3 following duties:

- 4 a. To exercise reasonable care in obtaining, retaining, securing, safeguarding,
 5 deleting, and protecting Plaintiffs' and Class Members' PII in their
 6 possession, care, custody, or control;
- 7 b. To follow their own policies and procedures and terms of service related to
 8 privacy and the protection of Plaintiffs' and Class Members' PII, including
 9 the PBI Defendants implementing the multi-layered security protocol,
 10 audits, evaluation, and stress-testing promised on their website;
- 11 c. To protect Plaintiffs' and Class Members' PII in their possession, care,
 12 custody, or control by using reasonable data security practices and
 13 procedures to protect that PII from reasonably preventable unauthorized or
 14 unnecessary disclosure; and
- 15 d. To implement reasonable practices and procedures to timely detect data
 16 breaches and other data security threats, and to timely take reasonable action
 17 act in response to such detection, including promptly notifying Plaintiffs and
 18 Class Members.

19 49. Defendants knew or should have known the risks of maintaining and storing PII, the
 20 importance of following published and industry-standard security protocols, and the importance of
 21 maintaining secure digital infrastructure.

22 50. Through Defendants' acts and omissions described in this Complaint, Defendants
 23 failed to provide adequate security to protect Plaintiffs' and Class Members' PII from being
 24 compromised, including by unauthorized access, disclosure, theft, and exfiltration.

25 51. Defendants breached their duties to Plaintiffs and Class Members by their acts and
 26 omissions, including by negligently, carelessly, and recklessly collecting, storing, transmitting,
 27 maintaining, and controlling Plaintiffs' and Class Members' PII, and by engineering, designing,

1 maintaining, and controlling systems that exposed Plaintiffs' and Class Members' PII to
 2 unreasonable risk of access and disclosure to unauthorized persons.

3 52. Defendants further breached their duties to Plaintiffs and Class Members in several
 4 ways, including by:

- 5 a. Failing to implement adequate and reasonable security systems, protocols,
 6 and practices sufficient to protect Plaintiffs' and Class Members' PII,
 7 despite the foreseeable risk of harm of failing to implement such systems,
 8 protocols, and practices;
- 9 b. Failing to comply with the minimum industry security standards for data
 10 security;
- 11 c. Failing to act despite knowing or having reason to know that Defendants'
 12 digital infrastructure contained the kind of flaw that lead to the Data Breach
 13 and was otherwise vulnerable to attacks; and
- 14 d. Failing to timely and accurately disclose to Plaintiffs and Class Members
 15 that their unencrypted and unredacted PII was accessed, viewed, disclosed,
 16 exfiltrated, and stolen by unauthorized third parties.

17 53. Defendants' breaches were a direct and proximate cause of Plaintiffs injuries and
 18 damages specified herein.

19 54. As a result of Defendants' negligence, Plaintiffs and Class Members suffered
 20 injuries and damages that include: (i) the lost or diminished value of their PII; (ii) out-of-pocket
 21 expenses associated with the prevention, detection, and recovery from unauthorized transactions,
 22 identity theft, and other unauthorized use of their PII; (iii) lost opportunity costs associated with
 23 expenditure of money, effort, and time to mitigate the consequences of the Data Breach, including
 24 but not limited to time spent deleting phishing email messages and cancelling credit cards; (iv) the
 25 continued risk to their PII, which can remain for sale on the dark web, where it is subject to further
 26 unauthorized access and disclosure; (v) future costs in terms of time, effort, and money that will be
 27 expended to prevent, monitor, detect, contest, and repair the impact of the disclosure of their PII
 28 because of the Data Breach, including ongoing credit monitoring.

55. These injuries, which also include an invasion of privacy rights, were reasonably foreseeable given the history of security breaches of this nature.

56. Due to Defendants' conduct, Plaintiffs and Class Members require and seek, among other things, extended credit monitoring. The Data Breach creates for Plaintiffs and Class Members an increased risk of identity theft and other types of financial harm. The consequences of identity theft are serious and long-lasting, such that there is an enormous benefit to early detection and monitoring. Plaintiffs further seek, in connection with this cause of action, all available relief specified below in their Prayer for Relief.

SECOND CAUSE OF ACTION

Violations of the California Consumer Privacy Act

(Cal. Civ. Code § 1798.150)

57. Plaintiffs re-allege each of the allegations set forth in the preceding paragraphs.

13 58. At all relevant times, each Defendant was a “business,” within the meaning of the
14 California Consumer Privacy Act (“CCPA”). Defendants operate in California and collect
15 consumers’ personal information. Each Defendant either has annual operating revenue that
16 exceeds \$25 million, annually collects the personal information of at least 50,000 California
17 residents, or derives at least 50 percent of its annual revenue from the sale of California residents’
18 personal information.

19 59. At all relevant times, Plaintiffs and Class Members have been “consumers” within
20 the meaning of the CCPA.

21 60. By the acts described above, Defendants violated the CCPA by negligently,
22 carelessly, and recklessly collecting, storing, and transmitting Plaintiffs' and Class Members'
23 "personal information" within the meaning of the CCPA, and by engineering, designing,
24 maintaining, and controlling digital infrastructure that exposed Plaintiffs' and Class Members'
25 nonredacted and unencrypted personal information to an unreasonable risk of unauthorized access
26 and exfiltration, theft, or disclosure. In doing so, Defendants violated their respective duties to
27 implement and maintain reasonable security procedures and practices appropriate to the nature of

Plaintiffs' and Class Members' personal information in Defendants' possession, custody, care, or control.

3 61. Plaintiffs have complied with the requirements of Cal. Civ. Code § 1798.150(b).
4 More than 30 days before the filing of this Complaint, Plaintiff Landi sent each Defendant a letter
5 by certified mail identifying the specific provisions that have been are or being violated by
6 Defendants, and no Defendant has cured the noticed violations. The Hurley Plaintiffs likewise sent
7 each Defendant a letter by certified mail identifying the specific provisions that have been are or
8 being violated by Defendants, but the required 30 days have not yet elapsed as of the date of the
9 filing of this Complaint. If Defendants respond to the Hurley Plaintiffs as they did to Landi, fail to
10 respond with 30 days, or otherwise fail to timely cure the noticed violations, the Hurley Plaintiffs
11 will likewise be entitled to and seek all relief available under the CCPA.

12 62. As a result of Defendants' violations, Plaintiffs and Class Members are entitled to
13 and seek all available relief specified in their Prayer for Relief below, including but not limited to
14 all available actual, statutory, and other damages, and injunctive relief.

THIRD CAUSE OF ACTION

Violations of the California Unfair Competition Law

(Cal. Bus. & Prof. Code § 17200, et seq.)

18 63. Plaintiffs re-allege each of the allegations set forth in the preceding paragraphs.

19 64. Plaintiffs and Class Members bring claims against Defendants under California's
20 Unfair Competition Law ("UCL"), which prohibits Defendants from engaging in any "business act
21 or practice" that is "unlawful" or "unfair." Cal. Bus. & Prof. Code § 17200, et seq.

22 65. Defendants engaged in “unlawful” business acts and practices by engaging in the
23 wrongful acts and practices set forth the in the First, Second, and Fourth Causes of Action in the
24 Complaint, including by failing to disclose the Data Breach to Plaintiffs and Class Members in a
25 timely manner.

26 66. Defendants' conduct complained of herein is also "unfair" under the UCL because
27 it violated and continues to violate established public policy of the State of California, and because

it was and is immoral, unethical, oppressive, or unscrupulous and causes injury to Plaintiffs, Class Members, and other consumers which outweighs its benefits.

67. As a result of Defendants' unlawful, unfair, or fraudulent business practices as alleged herein, Plaintiffs and Class Members suffered injury in fact and lost money or property, including but not limited to the loss of value in Plaintiffs' and Class Members' PII, the loss or impairment of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

68. On information and belief, Defendants' unlawful and unfair business practices and acts under the UCL are continuing in nature and have not been adequately cured since the Data Breach.

69. Plaintiffs and Class Members have no adequate remedy at law and thus, on behalf of themselves and the public, seek preliminary and permanent injunction relief against Defendants as set forth in the Prayer for Relief below.

70. Plaintiffs and Class Members further seek, whether in the alternative or in addition to damages sought in this Complaint under other claims for relief, all available restitution in an amount to be determined at trial, including the equitable disgorgement of any profits Defendants may have obtained as a result of their unlawful or unfair conduct.

71. Plaintiffs further seek, in connection with this cause of action, any and all further available relief set forth in the Prayer for Relief below, including but not limited to an award of their litigation costs, expert fees, and attorneys' fees under Cal. Code Civ. Proc. § 1021.5 and any other applicable law.

FOURTH CAUSE OF ACTION

Violations of the California Customer Records Act

(Cal. Civ. Code § 1798.82)

72. Plaintiffs re-allege each of the allegations set forth in the preceding paragraphs.

73. At all relevant times, Defendants were “businesses” under the terms of the CRA as sole proprietorships, partnerships, corporations, associations, financial institutions, or other groups,

operating in the State of California that owned or licensed computerized data that included the personal information of Plaintiffs and Class Members.

74. At all relevant times, Plaintiffs and Class Members were “customers” under the terms of the CRA as natural persons who provided personal information to Defendants for the purpose of purchasing or leasing a product or obtaining a service.

75. By the acts described above, Defendants violated the CRA by allowing unauthorized access to and disclosure of Plaintiffs' and Class Members' PII and then failing to inform them for weeks or months about the unauthorized access and disclosure thereby failing in their duty to inform their customers of unauthorized access and disclosure expeditiously and without delay.

76. As a direct consequence of Defendants' acts and omissions complained of above, Plaintiffs and Class Members incurred additional losses and suffered further harm to their privacy, including but not limited to the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and prevention of further loss and privacy injury that they would not have suffered if Defendants had timely informed them of the Data Breach.

77. As a result of Defendants' violations, Plaintiffs and Class Members are entitled to and seek all actual and compensatory damages according to proof, non-economic injunctive relief permitted under the CRA, and all other available relief sought in the Prayer for Relief below

FIFTH CAUSE OF ACTION

Declaratory Relief

78. Plaintiffs re-allege each of the allegations set forth in the preceding paragraphs.

79. An actual controversy over which this Court has jurisdiction now exists between Plaintiffs and Class Members and Defendants concerning their respective rights, duties, and obligations. There is a justiciable controversy over the legality of Defendants' acts, omissions, and practices complained of herein.

1 80. As a result of such practices, Plaintiffs and Class Members have been injured and
 2 will continue to be injured by Defendants' inadequate data security policies and practices and the
 3 continuing unremedied effects of the Data Breach. Therefore, declaratory relief is appropriate so
 4 that future controversies between the parties may be avoided by attaining judicial clarification of
 5 the parties' respective rights and obligations, including under any applicable laws or agreements
 6 under which Plaintiffs and Class Members may have enforceable third-party beneficiary rights.

7 81. Plaintiffs, therefore, seeks a declaration and related injunctive relief that (1) each
 8 Defendant's existing security measures do not comply with its explicit or implicit contractual
 9 obligations, law, and duties of care to provide reasonable security procedures and practices
 10 appropriate to the nature of the information to protect Plaintiffs' and Class Members' PII, and
 11 (2) to comply with their explicit or implicit contractual obligations, legal obligations, and duties of
 12 care, Defendants must implement and maintain reasonable security measures, including, but not
 13 limited to the following:

- 14 a. engaging third-party security auditors and penetration testers, as well as
 15 internal security personnel, to conduct audits, penetration testing, simulated
 16 attacks, and other testing on Defendants' respective digital infrastructure
 17 and software on a periodic basis, and promptly correcting any problems or
 18 issues detected by such third-party security auditors;
- 19 b. engaging third-party security auditors and internal personnel to run
 20 appropriate automated security monitoring;
- 21 c. auditing, testing, and training their security personnel on any new or
 22 modified security practices or procedures;
- 23 d. appropriately segmenting their software, digital infrastructure, and
 24 operations by, among other things, creating firewalls and access controls so
 25 that if the security of one area is compromised, unauthorized third parties
 26 cannot gain access to other segments of Defendants' software, digital
 27 infrastructure, or operations;
- 28 e. conducting regular database scanning and security checks;

- 1 f. routinely conducting internal training and education to inform internal
- 2 security personnel how to identify, contain, and respond to a security
- 3 breach;
- 4 g. offering free credit monitoring services to Plaintiffs and Class Members for
- 5 a period of not less than ten years;
- 6 h. educating Plaintiffs and Class Members about the threats they face as a
- 7 result of the disclosure of their PII to unauthorized third parties, and the
- 8 steps Plaintiffs and Class Members should take to protect themselves; and
- 9 i. storing and transmitting Plaintiffs' and Class Members PII in encrypted
- 10 form.

11 **VII. PRAYER FOR RELIEF**

12 82. WHEREFORE, Plaintiffs on behalf of themselves and Class Members pray for the
 13 following relief:

- 14 a. An order certifying the proposed Class and Subclasses pursuant to Rule 23;
- 15 b. An order appointing Plaintiffs and their counsel to represent the Class;
- 16 c. An order preliminarily and permanently enjoining Defendants from
- 17 engaging in the wrongful conduct alleged herein;
- 18 d. All declaratory relief set forth above;
- 19 e. An order requiring Defendants to offer Plaintiffs and Class Members free
- 20 credit monitoring and other appropriate protective services;
- 21 f. All available compensatory, statutory, and other available damages,
- 22 including punitive damages under Cal. Civ. Code § 3294(c)(3) and any
- 23 other applicable law, in an amount to be determined at trial;
- 24 g. Equitable relief requiring restitution and disgorgement of the revenues
- 25 wrongfully retained as a result of Defendants' wrongful conduct;
- 26 h. An award of their litigation costs, expert fees, and attorneys' fees under Cal.
- 27 Code Civ. Proc. § 1021.5 and any other applicable law;
- 28 i. Pre- and post-judgment interest as allowed by law; and

j. Such other relief as the Court may deem just and proper.

VIII. JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: July 31, 2023

COTCHETT, PITRE & McCARTHY, LLP

By: /s/ Andrew F. Kirtley

NIALL P. McCARTHY
ANDREW F. KIRTLEY
OWAIS M. BARI
GIA JUNG

RIGHETTI GLUGOSKI, P.C.

By: /s/ Matthew Righetti
MATTHEW RIGHETTI

WYNNE LAW FIRM

By: /s/ *Edward J. Wynne*
EDWARD J. WYNNE
GEORGE R. NEMIROFF

Attorneys for Plaintiffs and the Proposed Class

ATTORNEY ATTESTATION

I, Andrew F. Kirtley, am the ECF User whose ID and password are being used to file this Class Action Complaint. In compliance with Civil Local Rule 5-1(h)(3), I hereby attest that concurrence in the filing of this document has been obtained from each signatory.

Dated: July 31, 2023

By: *s/ Andrew F. Kirtley*
Andrew F. Kirtley